IET Networks

Review Article

Journals
The Institution of Engineering and Technology

read
有不少参考文献

Towards an incentive-compatible, reputation-based framework for stimulating cooperation in opportunistic networks: a survey

ISSN 2047-4954
Received on 25th April 2017
Revised 31st July 2017
Accepted on 14th August 2017
E-First on 11th October 2017
doi: 10.1049/iet-net.2017.0079
www.ietdl.org

Nikolaos Mantas[1], *Malamati Louta*[1] ✉, *Eirini Karapistoli*[1], *George T. Karetsos*[2], *Stylianos Kraounakis*[1], *Mohammad S. Obaidat*[3]

[1]*Department of Informatics and Telecommunications Engineering, University of Western Macedonia, Kozani 50132, Greece*
[2]*Department of Computer Engineering, Technology Education Institute of Thessaly, Larissa 41110, Greece*
[3]*Computer and Information Science, Fordham University, Bronx, NY 10458, USA*
✉ *E-mail: louta@uowm.gr*

Abstract: In opportunistic networks (OppNets), routing and data forwarding among mobile devices are facilitated by relays or next-hop forwarders. To guarantee end-to-end data delivery it is important to provide participation. However, in sparsely connected OppNets, it is extremely challenging to monitor the behaviour of the relays and identify selfish/malicious relays cooperating with each other in order to forge routing information or drop useful data. Cooperation enforcement schemes are seen as a lightweight alternative to conventional secure forwarding techniques that involve cryptographically signed certificate exchanges, providing a 'softer' security layer to protect basic networking operations. In general, cooperation enforcement schemes fall into two broad categories: trust establishment via a reputation system and pricing or credit-based schemes. This study offers a comprehensive survey of representative cooperation enforcement schemes that exploit a reputation system. The authors analyse their distinct features, identify and discuss critical challenges that should be efficiently addressed when designing such mechanisms, indicating at the same time potential solutions and provide an informative table to display the authors' findings. From this analysis, they examine issues and concerns surrounding the field of cooperation enforcement in OppNets, and provide guidelines and directions for future researchers.

可以作为参考文献//
这段

1 Introduction

Future communication systems will be increasingly complex, involving thousands of heterogeneous devices with diverse capabilities and various networking technologies interconnected with the aim to provide users with ubiquitous access to information and advanced services at a high quality level, in a cost efficient manner, any time, any place, and in line with the always best connectivity principle [1]. In this context, and taking into account the increasing volume of generated data, the stricter requirements for Quality of Service (QoS) and the special characteristics of wireless environments, the mobile *ad-hoc* networking paradigm and its evolutions may constitute a key enabler for the next generation wireless networks [2]. In particular, one of the most challenging research directions in the framework of *ad-hoc* networking is opportunistic networking.

In opportunistic networks (OppNets), which can be found in the literature under different names such as intermittently connected networks or challenged networks or delay/disruption tolerant networks, no assumption is made with regard to the existence of an end-to-end path between the source and the destination. The source and destination nodes might never be connected to the same network or at the same time. As a consequence, OppNets employ the store-carry-forward paradigm in order to enable nodes to exchange messages when a suitable forwarding opportunity occurs.

Due to their distinct characteristics, OppNets may be applied in various diverse domains that present the special requirements that fit with their design characteristics. For example, the applications of OppNets have been evolving from monitoring the behaviour of wild animals, like the Zebranet paradigm [3], to social-based applications such as information sharing and mobile crowdsensing systems in urban areas [4, 5]. Unfortunately, their proliferation has been rather limited as crucial features of OppNets, such as long end-to-end delays and frequent disconnections, lead to major challenges in message routing, mobility characterisation, quality of service provisioning and so on [6].

Besides these issues, security has emerged as an additional critical element in the network design and has since received considerable attention by researchers in the community of opportunistic networking. Similar to fixed networks, security in OppNets is examined from different viewpoints, such as confidentiality, integrity, availability, authentication, authorisation and non-repudiation. However, OppNets are generally more prone to security threats due to the absence of a complete path between the devices wishing to communicate, lack of any pre-established infrastructure, the absence of central control, lack of association, sharing of the wireless medium, dynamic topology changes and limited resource availability. In such a context, attacks from malicious nodes are hard to identify and defend. Thus, security is much more difficult to be established.

OppNets rely on node cooperation to perform and support basic functions such as routing and packet forwarding, a fact that increases the network performance sensitivity to nodes' misbehaviour [7]. In general, misbehaviour may be defined as any deviation from regular functionality, which may be unintentional, i.e. due to faults, transmission errors, node mobility and so on, or intentional, where selfish/malicious relay nodes wish to take advantage of certain situations. Intentional misbehaviour may be attributed to the nodes' selfishness to save their own resources (e.g. CPU, memory, battery) by not forwarding packets that are not directly of their interest (even though they expect other nodes to forward their own generated traffic), and to nodes' maliciousness that wish to harm and disrupt the normal operation of the network. Depending on the number of misbehaving nodes and their adopted strategies, throughput may be decreased, while network partitioning may occur. In any case, nodes' misbehaviour can significantly degrade network performance.

The exchange of digital, cryptographically signed certificates may be exploited in order to protect basic networking operations of OppNets. However, in many cases, the proposed models incorporating cryptographic schemes are considered to be complex and resource intensive. To this respect, cooperation enforcement schemes, a common term used for such approaches, are increasingly seen as a viable alternative aimed at providing a 'softer' security layer to these networks. Accordingly, the success of these systems highly depends on trust mechanisms that build the necessary trust relationships among relevant parties, thus, enabling them to automatically adapt their strategies to different levels of cooperation and trust.

Many studies about OppNets were published in the literature in the last decades. The main research activities focused on addressing routing and forwarding issues, since finding end-to-end routing paths in such disconnected environments is regarded as the most challenging issue [7]. On the contrary, trust and reputation, which are equally important in stimulating cooperation in OppNets, have attracted little to no attention. Currently, to the best of our knowledge, there is no prior effort in the literature providing a comprehensive overview of aspects and issues to be considered when designing mechanisms for promoting cooperation in OppNets. ? Most of the surveys are limited to a discussion on existing routing and forwarding protocols as well as on the related research challenges in the field, leaving cooperation enforcement out of their focus [8, 9]. Additionally, some surveys discuss on security and trust management solutions proposed in related research literature for OppNets, not however emphasising on cooperation enforcement mechanisms, but rather presenting them as one of the security aspect that should be considered besides authentication and access control, secure routing, privacy protection [10, 11]. Our aim is to cover this gap by identifying and discussing critical challenges involved in the design of reputation-based incentive compatible mechanisms for stimulating cooperation in OppNets, while revisiting current research efforts, providing a concrete analysis of their strengths and weaknesses and highlighting enabling technologies and solutions. Our ultimate goal is to contribute towards the definition of a commonly accepted incentive-compatible framework, by both providing a better understanding of the proposals published so far and pointing out relevant directions for future work.

On the other hand, trust and reputation is a relatively well-investigated field in a mobile *ad-hoc* networking setting. However, trust and reputation mechanisms designed for mobile *ad-hoc* networks cannot be readily applied to OppNets due to their specific characteristics. Overall, existing review articles either focus on addressing aspects of OppNets other than cooperation enforcement systems or are targeting mobile *ad-hoc* networks. Our work differentiates from the existing literature in several ways; (a) it examines recent works dealing with cooperation enforcement in OppNets from a system-level perspective, (b) it identifies and analyses issues and concerns surrounding reputation-based cooperation enforcement by elaborating on eleven potential pitfalls and (c) it summarises the multiple attributes of recent reputation-based cooperation enforcement systems in a table for better future referencing. While the field of reputation-based cooperation enforcement is quite broad, we hope that the analysis presented here will motivate more intensive future work in this area.

The remaining of the paper is organised as follows. Section 2 briefly overviews related surveys of the recent research literature and at the same time, highlight how our work differentiates from these studies. Section 3 gives a brief overview of trust and reputation including definitions, types, properties and measurement models. Section 4 surveys and analyses issues and concerns surrounding cooperation enforcement in OppNets with emphasis laid on reputation-based systems. Section 5 aggregates and discusses the findings of our work. Finally, Section 6 concludes the paper and highlights our future plans.

2 Related review works

Given the fact that trust and reputation are multidisciplinary concepts and have been around before the electronic age, these terms represent a well-studied area, while a wide variety of trust and reputation models with advanced features have been developed in recent years in a number of Information and Communication (ICT) research areas (e.g. pervasive systems [12], peer-to-peer networks [13], social networks and recommendation systems [14, 15], *ad-hoc* and wireless sensor networks [16], internet of things [17, 18] among others), which however lack coherence, as there is no consolidated set of well recognised principles that should be followed for building trust and reputation systems. There are general survey articles for reputation and trust. For example, Ruohomaa and Kutvonen [19] survey trust management in general, providing an overview on three aspects of trust: the concept of trust management, trust management models, and trust information models. Their survey focuses on trust initialisation and the evolution of trust in trust management systems.

A number of review articles exist that cover different aspects of trust and reputation in wireless *ad-hoc* networks. For example, Mejia *et al.* [20] analyse representative approaches for modelling trust in mobile *ad-hoc* networks. Specifically, the different tasks required by a trust model are identified (namely information gathering, information scoring and ranking, and action execution), while the way they are implemented under the perspective of information theory, social networks, cluster concept, graph theory and game theory is compared. It is found that the different approaches considered lack unity, while most of the models do not properly manage node reintegration in the system.

Azer *et al.* [21] survey trust and reputation schemes for *ad-hoc* networks, focusing on the goals, features, and architectures of the trust management system for such networks. Similarly, Yu *et al.* [22] examine the latest methods that have been proposed by researchers to manage trust and reputation in wireless communication systems. Marias *et al.* [23], after briefly revisiting potential attacks in the network layer of wireless *ad-hoc* networks as well as conventional security and authentication methods, survey the most important cooperation enforcement schemes that have been introduced up to that date providing a comprehensive comparison between them. Specifically, they categorise the proposed schemes into reputation and credit-based schemes. The first category is further divided into systems that are based only on direct (first hand) information and to systems that additionally exploit indirect (second hand) information. They further divide the second category to systems requiring tamper-proof hardware usage and to systems offering trusted third party (TTP) to the nodes. The surveyed schemes are compared with respect to robustness against misleading nodes, robustness against collusion, usage of global or context dependent reputation values, utilisation of cryptographic techniques and exploitation of promiscuous mode of operation. Similarly, in [24], the authors after presenting a number of representatives reputation-based schemes in the context of *ad-hoc* networks, they analyse their distinct features and discuss on their relative merits and weaknesses. The authors conclude that the proposed schemes lack unity, while it is very hard to comparatively assess the performance of the different proposed schemes.

可以用来支撑我的论据

防篡改硬件或者第三方

In the context of OppNets, Chakchouk [7] presents the main building blocks of related opportunistic routing mechanisms. Subsequently, the different routing schemes are classified based on different objectives, optimisation tools employed and approaches used. The authors only slightly touch upon privacy and security issues, by briefly revisiting security-aware related works in the context of opportunistic networking. In [6], and in the context of cooperative delay-tolerant networks, the authors refer to the main issues involved, namely, the impact of different degrees of nodes' cooperation to the network's performance, the detection of non-cooperative nodes and the design of protocols that impose nodes' cooperation including reputation-based, credit-based, game-theoretic-based and barter-based schemes. Similarly, in the context of vehicular networking, Benamar *et al.* [25] classify incentive-based cooperative forwarding schemes into three main categories: barter-based algorithms, virtual currency-based and reputation based. In [10], Wu *et al.* after elaborating on security threats and requirements, they provide a security architecture of OppNets, discussing on authentication and access control issues, secure routing, privacy protection, trust management and overviewing representative cooperation incentive mechanisms.

In a similar line of works, a number of related surveys focus on incorporating social aspects in the design of OppNets. For example, in [8], the authors present a comprehensive survey of recent social-aware routing protocols, which exploit social relationships to design efficient routing protocols. They emphasise on social behaviour and interactions among nodes and analyse design related issues, such as sources of social information, metrics and approaches that could be adopted so as to identify/characterise social ties and optimisation strategies for improving the performance of social-aware routing protocols. As noted, even though most delay tolerant networking routing algorithms assume that nodes are willing to forward messages for others, the impact of selfishness on performance is characterised as an interesting research challenge. The authors constrain selfishness to the social-based one, where a node may discard the message received from those with whom it has no social ties, while they refer to some forwarding algorithms that consider reputation-based schemes or credit-based approaches so as to stimulate nodes' cooperation. In [9], the authors summarise the social properties of delay tolerant networks and discuss on social-based routing approaches proposed in recent related research literature, taking advantage of either positive social characteristics (such as friendship, community, centrality) or negative social characteristics, such as selfishness. Specifically, after acknowledging that traditional incentive mechanisms introduced in wireless *ad-hoc* networks do not work well in a Delay Tolerant Networking (DTN) context, they categorise existing incentive mechanisms for DTN routing in three categories: reputation-based, tit-for-tat-based and credit-based schemes. In [26], the authors focus on social-aware schemes that exploit social information derived from opportunistic encounters so as to improve data forwarding. An updated taxonomy is provided for opportunistic routing including a sub-category related to social similarity, which is further divided into community detection, shared interests, nodes' popularity and user dynamic behaviour in different time periods of the day. However, the authors do not refer to any issues concerning selfishness, cooperation and incentive provisioning. In [27], the authors propose three trust metrics: Social Trust, in which trust is established through trusted/friendly social connections, Environmental Trust, in which trust is inferred from careful observation and community detection of the surrounding peers and Similarity Trust, in which trust is based on similarity/taste of different users. Reputation systems are constrained to trust estimation based only on direct interactions. All metrics can be combined and used in parallel.

Several literature reviews have focused on one important aspect of reputation and trust, namely the robustness against attacks. Hoffman *et al.* [28] focus on attacks and defence mechanisms in reputation systems, categorising attacks as: self-promoting, whitewashing, slandering, orchestrated and denial of service. Kerr and Chon [29] implement a number of cheating strategies against a few established trust systems, demonstrating that all the tested systems are vulnerable to at least one type of premeditated attack from dishonest participants. Jøsang and Golbeck [30] discuss nine different types of attacks on trust and reputation systems, identifying the need for either a standard set of metrics for measuring the robustness of a trust system or some standard techniques for the theoretical robustness analysis of trust systems.

To the best of our knowledge, there is no prior related research work that focuses on reputation-based cooperation enforcement in the context of opportunistic networking. Following, we identify and discuss on issues and concerns surrounding reputation-based cooperation enforcement systems and present and analyse critical challenges involved in their design.

3 Reputation-based incentives in OppNets

Reputation-based mechanism design for promoting cooperation involves trust, reputation, trustworthiness and well-behaving as well as misbehaving nodes acting in an opportunistic networking setting. Because of this interconnection, we begin by providing some definitions on these terms, and then we classify the reviewed models having these notions in mind.

3.1 Trust, reputation, trustworthiness and misbehaviour

Trust is often described as the belief of an entity in the competence and benevolence of another entity to act honestly, reliably and dependably. We follow the definition of trust (or symmetrically distrust) as given in [31]: 'a particular level of subjective probability with which an agent assesses that another agent or group of agents will perform a particular action both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action'. The authors add 'when we say that we trust someone or that someone is trustworthy, we implicitly mean that the probability that he will perform an action that is beneficial or at least not detrimental to us is high enough for us to consider engaging in some form of cooperation with him'. Reputation is an assessment of the performance of the node and, according to our perspective, it constitutes a metric for establishing trust relationships. In general, reputation is subjective, non-symmetric, dynamic and context dependent. The reputation of a node increases when it carries out rightly the task of forwarding the packets that are dispatched by its neighbours, without altering their fields.

The nodes' trustworthiness reflects each time the current behaviour of a node either as a member of the network or as a witness of other nodes' functionality. As such, it is an attribute that may be viewed in the context of network operation (e.g. a node is trustworthy if it consistently forwards received packets, that is a node dropping packets is characterised as untrustworthy) and in the context of the functionality of the reputation mechanism (e.g. a node constitutes a trustworthy witness if it consistently provides requesters with nodes' reputation ratings that reflect the real picture concerning their behaviour with respect to network operation). Nodes' trustworthiness in both contexts should be dynamically updated so as to reflect each time nodes' behaviour. Misbehaviour, similar to trustworthiness, is a node's attribute indicating intentional or unintentional deviation from regular functionality. Thus, mechanisms should be provided for identifying and/or addressing unintentional misbehaviour (e.g. in case a node is believed to have unintentionally misbehaved, its trustworthiness level modification should be accordingly outweighed), while wireless medium vulnerabilities should also be taken into account (e.g. potential low quality of the wireless link or transmission collisions resulting in packet loss – especially in heavy network loads).

Finally, after surveying various schemes proposed in related research literature, we could not identify a common definition on nodes' selfishness. Generally, selfish nodes drop packets so as to conserve their own resources (e.g. energy), while malicious nodes attack networks in order to disrupt its normal operation. However, selfish nodes in different research works are attributed with different behaviour. In [32], even though the authors consider that a selfish node does not want to spend its own resources forwarding packets that belong to different nodes, they claim that selfish nodes strive to be unattractive so as not to be selected as potential forwarders. However, in case they are selected, they will forward the packets. In [33], selfish nodes are willing to forward messages for nodes with whom they have social ties, but not for others. In [9], selfishness is distinguished as follows: individual selfishness, where each node exhibits the same degree of selfishness to every other node and to social selfishness, where a selfish node exhibits different levels of selfishness to different group of people.

3.2 Classification of cooperation enforcement schemes

In general, cooperation enforcement schemes for wireless *ad-hoc* networks fall into two broad categories: (a) trust establishment by means of reputation systems, and (b) pricing/credit-based schemes. Reputation mechanisms establish trust by exploiting learning from experience concepts in order to obtain a reliability value of the system's participants in the form of ratings based on observations, past experiences and other entities' view/opinion [34]. In general, reputation-based systems are considered to sustain rational cooperation and serve as an incentive for good behaviour because good players are rewarded by the society, whereas bad players are penalised, while the reputation ratings are seen as a predictor of future behaviour of the system's participants. Pricing and credit-based schemes on the other hand, provide economic incentives for collaboration by charging as well as rewarding service usage and provision [35, 36]. These schemes require tamper-proof hardware

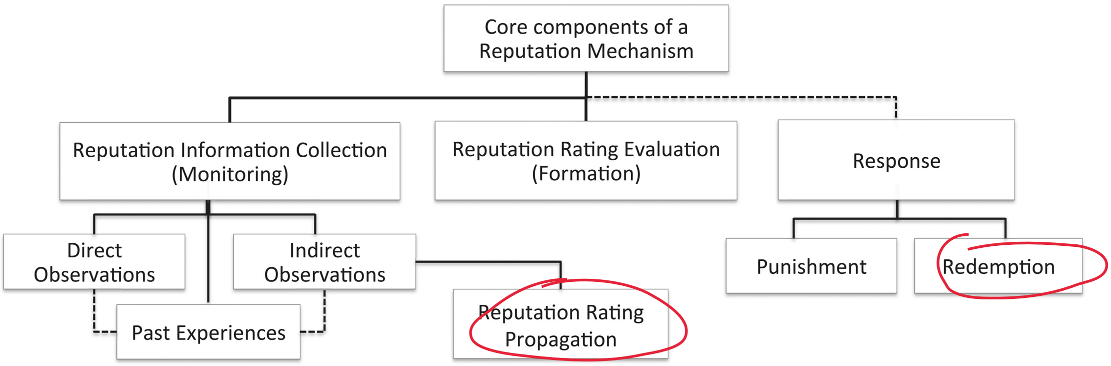
Core components of a Reputation Mechanism
Reputation Information Collection (Monitoring)
Reputation Rating Evaluation (Formation)
Response
Direct Observations
Indirect Observations
Past Experiences
Reputation Rating Propagation
Punishment
Redemption

Fig. 1 *Core components of a reputation-based scheme*

也是tit-for-tat ???

existence or exploitation of trusted third-party services. Both these categories can interact with secure routing protocols, so as to comprehensively protect a network (even though the complexity in such a case would be increased). Some schemes utilise both reputation mechanism and economic incentives, forming hybrid solutions [37]. Additionally, several schemes are inspired from game theory, where payoffs are assigned to different node strategies [38, 39]. Finally, some schemes exploit barter-based strategies so as to deal with selfish nodes. For example, in [40] a community-based incentive barter scheme is exploited to deal with selfish behaviour of some nodes in socially aware networking. In this scheme, a node contributes to a community by providing forwarding services to its members and gets the same amount of services from nodes in that community, incentivising community members to cooperate, thus enhancing message exchange probabilities. Additionally, in [41], according to the proposed Social Contribution-based Routing (SCR) protocol, the candidate node for relaying the packet is the one with the higher delivery probability (determined on the basis of the contact frequency between the relay and the destination) and the smaller social contribution. In SCR, social contribution includes both reciprocal contribution and community contribution, defined as the forwarding services that the node provides for other nodes (i.e. either to those encountered or to the nodes within the same community, respectively). A node is permitted to select a relay node with a little more social contribution than itself. Thus, social contribution in SCR plays the role of incentives. Similarly, in [42] the authors employ a tit-for-tat mechanism to deal with selfish node behaviour, albeit in the context of a content exchange protocol.

Focusing on reputation systems, their usefulness highly depends on their underlying trust framework and model, e.g. information gathering and representation, analysis and reasoning, reputation/trust value computation, decision making and action performed. In [43], the authors describe a framework for reputation systems comprised of a monitoring component (with the goal of gathering first-hand information about the behaviour of the nodes in the network), a reputation system (serving as an incentive for good behaviour and providing a basis for the choice of prospective transaction partners), and a response mechanism, which aims at isolating nodes that are deemed misbehaving by not using them for routing and forwarding and also denying them service. The features of the reputation systems are classified in accordance with the representation of information (i.e. how monitored events are stored and translated into reputation ratings), use of second-hand information (i.e. information obtained from other nodes), trustworthiness (i.e. how to build and represent the reliability of a node acting as a witness to provide honest feedback concerning its experiences), redemption as well as the secondary response (i.e. mechanisms that ensure that a node misbehaving in the past can participate again in the network in case it exhibits good behaviour, punishing it however by responding quicker to a recurring bad behaviour).

The categorisation and classification of the existing reputation systems that appear in the literature is depicted in Fig. 1. As it can be seen, reputation-based schemes support effective mechanisms to evaluate the reputation of other nodes of the network (denoted by reputation rating evaluation (formation)). A number of them incorporates response techniques that isolate misbehaving nodes, i.e. those that show a low reputation value, enabling them however to re-access the system in case they exhibit good behaviour in the future. Regarding the reputation information collection mechanism, the reputation-based schemes can be further divided into two subclasses. The first subclass includes schemes according to which the nodes are only based on their personal observation of the behaviour of their neighbouring nodes (first-hand reputation information), including their own past experiences with other nodes to take a routing decision. The second category includes schemes according to which the nodes take into consideration the observations of other nodes in the network (second-hand reputation exchanges). The nodes in these schemes exchange information relative to reputation values. If a node observes that another node does not behave rightly, then it reports this observation to other network nodes. The schemes that belong in this subclass also deploy an effective mechanism to distribute this information (denoted by *reputation rating propagation*).

4 Design aspects and operational characteristics of current reputation systems

In this section, we provide a comprehensive list of aspects and issues to be considered when designing a reputation-based, cooperation enforcement mechanism. To the best of our knowledge, such an in-depth analysis is missing, and even though we could not argue that this list is exhaustive, it covers all critical issues identified. Additionally, the authors provide their proposals and insights on how to employ and exploit several of the identified aspects.

reputation机制 进行深入的分析//
blackhole比例强度->network性能
Prophet强度的 视为lambda 采用 uniform分布建模 高斯分布建模

4.1 Monitoring

Of fundamental importance in designing a reputation system is the reputation monitoring mechanism. The reputation information collection mechanism may be based (a) on direct experiences of the evaluator node with the target node, (b) on direct observations of the evaluator node concerning target node's behaviour with respect to other nodes' transmissions and (c) on propagated reputation information on the target node's past behaviour. (a) and (b) Constitute first-hand information, while (c) is referred to as second-hand information. Some of the reputation mechanisms in related research literature, e.g. [44], gather first-hand information by deploying the promiscuous mode of operation on each node, i.e. the evaluator node may listen to its neighbourhood nodes' transmissions and see if a packet to be forwarded by the target node has been forwarded or not. Such a mechanism implies the existence of omnidirectional antennas and assumes symmetric bi-directional links. Usage of power control schemes and directional antennas so as to improve capacity, constitutes monitoring a very difficult issue to handle in the design of reputation mechanisms. Additionally, by overhearing the transmissions of adjacent nodes, a node cannot be sure that the forwarding node has reached the next hop or the destination, as it fails to capture potential transmission errors. Furthermore, such a mechanism cannot efficiently address the 'store-carry-forward' principle adopted in an OppNet setting.

依赖ack

In the light of the aforementioned, most of schemes proposed (including [44]), adopt a different procedure in order to effectively address long delays and intermittent communication. Specifically, the most widely used monitoring mechanism is based on the deployment of a watchdog mechanism [45, 46]. The Watchdog counts the arrival of acknowledgement packets (ACKs) that are generated at the destination, when data are received. Normally the ACKs are routed back to the data source along the same transmission path. Such an approach assumes slow mobility and the existence of the contemporary routing path between the source and the destination. However, such a mechanism is not efficient (if at all feasible) in OppNets due to frequent network partitions. Thus, there is a challenge on how to design an efficient Watchdog mechanism without assuming the existence of the contemporary end-to-end routing paths and slow mobility. To overcome these limitations, a positive feedback message (PFM) [46], which helps the Watchdog component to effectively monitor the forwarding behaviour of a forwarding node, is proposed. PFM is created by a third node and aims in reassuring the source node that the intermediate node has really helped in data delivery.

However, relying on other nodes for monitoring the forwarding behaviour in order to build reputation is quite risky in OppNets, as routes are quite dynamic and neighbours are not always available to monitor the behaviour of one another. A more appropriate approach in such an environment is for each node to monitor all the transactions that are involved into and exchange the collected data when it gets in close proximity with other nodes in social or other bounds. Such a monitoring framework for reputation building is described in [47].

An important aspect in this framework is authentication and identity management that will ensure the validity of the exchanged messages. In OppNets the authentication procedure cannot take place in an interactive way since we have an intermittent network environment. On the other hand cryptography-based authentication cannot be implemented without relying on a third party that provides the respective keys for all nodes that will possibly interact. This holds for either identity-based cryptography or traditional public key cryptography. Since the key provider cannot be always reachable, a possible solution is for all nodes to acquire their authentication keys before entering the network [10, 48].

The monitoring mechanism itself raises the issue of fairness and the problem of distinguishing between unintentional and intentional misbehaviour. These issues should be carefully considered, as otherwise, a collaborative node will in some cases lose its reputation and be considered as misbehaving.

4.2 Rating formation and types of information considered

As analysed before, the rating formation of a node under evaluation may be based on direct experiences of the evaluator node with the target node, on observations of the evaluator node concerning target node's behaviour or on propagated reputation information on the target node's past behaviour. On the one hand, reputation rating formation exclusively based on direct experiences and observations increases the time required for a misbehaving node to be identified. Quite the contrary, considering honestly reporting nodes, the more information a node is taking into account, the faster and more accurate the rating estimation will be. Thus, malicious and selfish nodes may be identified faster (even at remote locations), before affecting network operations, leading to a robust solution. On the other hand, reputation rating formation exclusively based on indirect information may prove costly if the propagated information is inaccurate. In any case, disseminating reputation information increases the network overhead as well as the storage and computation requirements of the nodes. Other issues that arise in forming the reputation of a node are analysed below.

4.3 Rating formation and inaccurate information

OppNets constitute a highly dynamic, variable and uncertain environment. Truthful information dissemination cannot be automatically assumed. Thus, special care should be taken when inaccurate reputation related information is offered to the decision making process and potentially disseminated to other nodes. Inaccurate information may occur unintentionally or intentionally. Considering the first case (unintentional inaccurate information provisioning), according to our view, two parameters should be considered; the number of interactions/observations of the behaviour of a specific node as well as the number of the involved packets, reflecting the confidence of the evaluator node in the target node's rating while being formed. Specifically, it is quite safe to assume that nodes that have been involved with the target node only a few times would not have formed an accurate measure regarding its behaviour. Additionally, if the reputation ratings are formed on the basis of a small number of packets, there is a possibility that they do not reflect the real picture. In case a node is believed to have unintentionally provided inaccurate information, its trustworthiness modification should be accordingly outweighed.

On the other hand, intentional inaccurate information provisioning in the form of spurious reputation ratings (attributed to either fraud/false praises or bad mouthing/false accusations) should be considered and mechanisms should be provided in order for their impact to the overall network performance to be mitigated. Considering specific punishment mechanisms, denial of service to misbehaving nodes may result in various degrees of network partitioning. While this could be avoided by propagating positive ratings, there exists the danger of fraud, crediting misbehaving nodes.

In general, a mechanism for eliciting true feedback in the absence of TTPs is necessitated. According to the simplest possible approach that may be adopted in order to account for possible inaccuracies in the information provided by the witnesses' nodes (both intentional and unintentional), the evaluator nodes can mostly rely on their own experiences rather on the target node's reputation ratings provided by witnesses. To this respect, a node's reputation rating provided by witness nodes may be attributed with a relatively low significance factor. Our proposal is to exploit the concept of node's trustworthiness in the context of reputation mechanism functionality, incorporating the latter in the overall reputation rating formation process. Specifically, reputation ratings may be formed by means of a weighting function formulated so as recommendations originated from honest reporting nodes are attributed with higher significance factor, whereas reports (positive or negative) propagated from untrustworthy nodes have a small impact on the formation of the node's reputation ratings. Even though such a concept has already been adopted in related research works, e.g. [33, 44], they all consider a good behaving node in the context of network operations as an honest reporting node, which is not necessarily the case. Additionally, there is no distinction between intentional and unintentional inaccurate information provisioning.

降低虚假证据的影响权重

Considering both the aforementioned cases, i.e. taking into account intentional and unintentional second-hand reputation related information when estimating a node's ratings value, we propose to introduce a reputation rating credibility metric, reflecting both the recommenders' trustworthiness in the eyes of the evaluator and the recommenders' confidence in the reputation rating provided on the basis of first-hand information that it owns. The reputation rating credibility metric should not be predefined. Instead, it should be dynamically formed in order to illustrate the current picture concerning feedback provision in a truthful and accurate manner.

4.4 Rating formation and oscillating behaviour

振荡行为

Node's consistent good behaviour should be reflected and rewarded as malicious nodes may strategically alter their behaviour for maximising their benefit. For example, a node may start to behave maliciously after it has attained a high reputation value (i.e. collaborating for a specific period of time) or it may exhibit an oscillating pattern (being fully collaborative or honest for a period of time and fully malicious for the next period and so on, or even adopting a random pattern) so as to avoid detection. Even if this behaviour is more difficult to identify, we believe that when detected it should be severely punished. In [49], the main target is to cope with nodes that alter their behaviour with time. Specifically, the routing protocol presented is based on a reputation

采用grayhole方案来应对

value calculated via two specific mechanisms, i.e. the acknowledgement-based reputation system and the message delivery reputation system. In this way, a reputation threshold is defined that is used to indicate misbehaving nodes.

4.5 Rating formation and time effects

我不确定？？？如果更近的影响更大，如何应对振荡呢？

In order to further improve the correctness of the reputation rating assessment, taking into account that nodes exhibit non-deterministic behaviour, time effects should be introduced in the mechanisms so as to model the fact that more recent events should weigh more in the evaluation of the target node's overall reputation rating by the evaluator. Thus, potential modifications of the target nodes' behaviour in recent past that affect recommendation accuracy may be addressed by considering the time the last interaction/observation occurred and outweighing accordingly the significance attributed to the specific recommendation. Some of the reputation/trust mechanisms presented in related research literature (e.g. [32, 33]), consider reputation aging. However, in a number of them (e.g. [32]), reputation aging corresponds to nodes' punishment in order to address cases where packets are undelivered and the nodes cannot verify if this is attributed to the misbehaving behaviour of a node(s) in the routing path (and which node(s) exhibited such a behaviour) or if this is attributed to another reason (e.g. a fault).

4.6 Rating formation and the cold start problem

An important issue in reputation rating formation is the cold start problem. A new, not known to the network, node should be attributed with an initial reputation value to be updated on the basis of either direct or indirect (gathered) experiences. Various approaches adopt solutions that might be unfair to several system participants. A popular approach is to assign neutral or default reputation values to new nodes entering the system. This solution however, can favour either existing participants or newcomers depending on the underlying model considered for building the reputation values. High initial reputation values provide incentives for changing identities so as to wipe out possible bad behaviour in the network ('whitewash'), while on the other hand, low initial values in such dynamic networks raise the difficulty of quickly reaching an accurate picture concerning a node's behaviour. For example, let us consider the case of a collaborating node being attributed with a high reputation value in a specific network segment. In a specific point in time, it moves to another segment in which it is unknown and the policy adopted for newcomers is to be attributed with a low initial reputation value. This punishment approach (even if it is considered in some contexts a better alternative) would result in constraining packets from being forwarded through the best possible relay in the context of wireless *ad-hoc* networks. We believe that initial reputation values should be adaptively chosen, taking also into account social characteristics/relations of nodes (as in the case of [44]). This may be considered as a better alternative in terms of accuracy and fairness.

4.7 Reputation rating propagation

传播

In working with second-hand information, the majority of the reputation systems in the context of OppNets acquire reputation-related information by exchanging related records when two nodes meet. In the context of reputation rating propagation, the following issues should be carefully considered; (a) to which nodes should reputation related information should be propagated (e.g. none, neighbourhood structure, nodes comprised in a 'friends' list, nodes' within a certain community, the whole network etc.), (b) when and how often should reputation information be propagated (e.g. every time a misbehaviour is identified, at pre-specified time intervals, after a specific number of events has taken place) and (c) what type of reputation related information should be propagated (e.g. an alarm message identifying a misbehaving node, positive and/or negative reputation related information, reputation ratings formed on the basis of nodes' experiences, aggregated or not reputation ratings corresponding to a specific time-period or by the whole history). The critical parameter should always be the overhead introduced in conjunction with the resource constraints imposed. When deciding on the aforementioned aspects, nodes' mobility should be considered as well, since node movement can increase the scope of direct interaction and recommendation propagation, and as such, speed up trust convergence.

4.8 Response: punishment and redemption

Different approaches concerning actions taken after identifying a misbehaving node are proposed in related research literature. Some mechanisms do not punish misbehaving nodes, as their generated traffic can still be handled by the network, while these nodes are avoided during path selection procedures, so as to ascertain that nodes obtain good services; misbehaving nodes are not used in the path, reducing the overall effect of misbehaviour. However, by doing this, nodes are not provided with an incentive to behave well so as not to possibly face denial of service. Most of the proposed schemes gradually isolate the node from the entire network or from a specific network segment (depending on the degree of the second hand information dissemination) after its reputation falls below a pre-specified threshold that will characterise it as misbehaving.

Most systems have a punishment component for misbehaving nodes. The isolation of the misbehaving nodes is done in two steps: first, these nodes are avoided during packet routing, and second, they are denied cooperation when they request it. While many mechanisms exclude nodes from the network forever depriving them the opportunity to participate in the network again, only few systems provide a forgiving mechanism (referred to as secondary chance/response or redemption mechanism), giving a bad node the opportunity to become a member of the network again. The forgiving mechanism may be seen as a solution either when the network cannot discriminate between intentional and unintentional misbehaviour, or when parameters, such as the time-varying, unreliable and asymmetric characteristics of the wireless links, are not taken into account. In most cases, the proposed schemes incorporating a forgiving mechanism do not provide many details with respect to its design, while in general they state that a misbehaving node is allowed access to a network in case it starts to exhibit good behaviour for a period of time.

少部分系统提供变好的机会

The authors' view on this issue is the provision of a redemption mechanism, with the simplest approach being the allowance of nodes' re-entrance after a specific time period of exclusion or after the completion of a specific number of events. However, attention should be given to the definition of the number of events and/or the time period, in order not to constitute a disincentive for honest behaviour. Furthermore, mechanisms could be added for punishing more severely a recurring bad behaviour (e.g. respond quicker to a bad repeated behaviour). Concerning the punishment method introduced, we believe that a less severe/strict punishment, at least till a certain reputation value threshold is reached, could serve as an incentive for good behaviour, without excluding completely a node from the network, being at the same time more robust to specific collusive behaviours resulting to network partitioning. For example, an intermediate forwarding node may handle up to a specific portion of a node's generated traffic, which should be closely connected to its attained reputation value, or in case a QoS-aware routing protocol is exploited, the packets received may experience delay proportional to the attained reputation of the previous hop.

赎回机制

我们要不要考虑概率性地拒绝转发？？

4.9 Other important design issues

4.9.1 Reputation and context: Trust in general is assumed to be context-specific and it can be viewed as global or personalised. Accordingly, it is believed that the formal definition of reputation should be a context dependent process, relying on contextual features, societal values and environment goals of the target domain, where reputation is being defined and deployed. Some researchers view different contexts as different service categories (e.g. packet forwarding, routing in the wireless *ad-hoc* domain), while others estimate reputation ratings considering different dimensions of trustworthiness (e.g. quality, delivery time, guarantee and price). Ratings from the same context (or at least from similar contexts) and their relationship should be taken into account when calculating trust values.

The independence of reputation formalisation in different contexts on the one hand and the effect of reputation in conceptually related contexts on the other hand, complicate the development of a global reputation value for each entity in a multi-context environment. Marias *et al.* [23] believe that an aggregated value allows a node to hide its misbehaviour with regard to an operation, and thus, the aggregated value does not reveal the importance that is given to different tasks. On the other hand, the authors in this study, believe that treating nodes' trustworthiness with respect to network operations as a behavioural aspect, independent of the operation considered, in essence relieves the reputation mechanism of evaluating the node's offering with respect to the specific operation considered according to the evaluator's personalised preferences, desires and constraints. This way, the reputation mechanism would not have to take into account personalised preference similarity measures among the nodes, leading to an accurate picture of the nodes' behaviour in a time efficient manner, without consuming the limited resources of nodes in an opportunistic networking context. Additionally, in case the contexts are related (i.e. different network applications), the actions taken when identifying misbehaviour are similar, even though the scope of misbehaviour may be different (e.g. ranging from not forwarding for resource reservation or from simple selfishness, to active attacks aimed at denial of service and subversion of traffic).

trust 独立于具体的 netw op

4.9.2 Reputation and social aspects: Reputation in information systems has been binded with social dimensions in the past. For example, Sabater and Sierra [50] present REGRET, a reputation system that exploits, among others, the social relations between agents so as to efficiently estimate reputation in case interactions in large multi-agent societies are scarce. Pujol *et al.* [51] establish reputation in relation with the position of each member of a community within the corresponding social network. An algorithm called NodeRanking is proposed for creating a ranking of reputation ratings of community members by means of the social network graph.

Lately, social relations among nodes are exploited in OppNets in order to improve the decision on the best relay node and the best time to forward information to. This is attributed to the observation that people with close relationships (family, friends), sharing similar interests or even belonging within the same community tend to interact more often, more regularly and for longer periods than others. A large number of the so-called social-aware routing protocols have been presented in related research literature [7, 8], where, in most cases, the next relay node for message transmission is determined on the basis of forwarding capability and trust. Friendship, similarity, community, centrality are some of the social metrics considered when designing message forwarding protocols for OppNets.

An emerging research area lies in exploiting both users' relationships in online social networks and users' offline connections and interactions in opportunistic/spontaneous networks and location-based social networks, so as to optimise information dissemination in wireless *ad-hoc* networks [52]. In [53], online and offline communities are seen as complementary and correlated. A cross-community sensing and mining framework is proposed, aiming to connect heterogeneous communities. However, identifying human behaviour patterns by analysing data sensed and collected from multi-community environments in the cyber-physical space still presents major research challenges.

Social ties have also been introduced in incentive mechanism design for promoting cooperation in OppNets. Some works utilise social characteristics of nodes in order to determine a composite trust metric and establish trust relations [44], others exploit the notion of community for reputation propagation so as to establish trust in a time efficient manner [54, 55], while others consider an initial reputation value based on the social relations of nodes [56]. Finally, some schemes [40, 41] allow a node to forward packets to a relay only if the forwarding services it has provided to the considered node or to nodes belonging in its community are the same or slightly less than the ones provided to itself by the relay or the members of the community.

Social-aware incentive mechanisms in the opportunistic networking context are still in infancy, while several challenges should be efficiently addressed. As noted in [9], a challenging task is how to accurately extract social related information in OppNets due to lack of continuous connectivity and time-varying topology. Additionally, combination of multiple social metrics is possible and may lead to performance improvements, even though the decision on which metrics to consider and in which context is not a trivial task. Furthermore, one should carefully consider the trade-off between performance and complexity [8, 9].

4.9.3 Information representation storage requirements: The reputation ratings may either adopt a continuous measure of a binary/Boolean form or may lie in a specific range value incorporating positive and/or negative values. Moreover, all experiences may be stored or only those corresponding to a specific history window (e.g. the most recent). The latter design choice also raises issues such as how this history window is determined and so on. One should keep in mind that the reputation mechanism comes at the cost of keeping reputation related information at each node for some time, and updating it after a specific event is observed, a fact that places implications on the overall design given the resource-constrained nature of OppNets.

5 Comparison

From the above analysis, which has introduced most of the work undertaken in the area of cooperation enforcement in OppNets, it can be deduced that researchers are using many types of methodologies borrowed from different domains to calculate reputation. Table 1 shows a comparative evaluation of the studied reputation-based schemes using the classification criteria defined in Section 4. The table summarises, among others, the types of observation used towards modelling reputation, the different forms of reputation propagation adopted, the mechanisms used to update reputation as well as the robustness exhibited against different types of attacks.

At the top level of our comparative evaluation, we have divided the cooperation enforcement schemes between approaches that perform some form of reputation monitoring and schemes that do not. As it can be seen from Table 1, the vast majority of the surveyed studies incorporate a monitoring component for effectively assessing a nodes' forwarding competency. Specifically, besides gathering first-hand information by deploying the promiscuous mode of operation, an enhanced watchdog mechanism that relies on feedback messages created by nodes that overview data exchanges between a source and a destination is one of the most popular approaches used to monitor the behaviour of a forwarder. This is because watchdogs alone are not feasible implementations in OppNets and require certain conditions to hold since such deployments are prone to frequent partitions and exhibit high mobility. Other approaches introduce a periodically available Trusted Authority (TA) to help monitor a node's reputation [58]. At this point it should be noted that in a number of the surveyed papers [55, 37], nodes locally store their own reputation evidence that is relayed upon request and in this respect a monitoring component is not necessitated.

Another critical observation is that almost all studies rely on both direct and indirect observations to model reputation. Second-hand information is exploited towards building reputation through adopting a form of reputation propagation in the network. The vast majority of the examined schemes consider the exchange of reputation-related information when two nodes meet (through encounters), others are based on recommendations, some share reputation values in the same social community, while others enable reputation evidence relaying on demand. Based on the gathered forwarding evidences, nodes make decisions on the trustworthiness of individual nodes and in the sequel take appropriate forwarding decisions. However, there are several disadvantages in using indirect information that may lead to wrong and costly forwarding decisions. Thus, in [32], a local notion of reputation is adopted in order to avoid the overhead imposed and the technical complications of reputation propagation. Finally, concerning the reputation update mechanism, in most studies, reputation is increased/decreased either linearly upon successful/unsuccessful forwarding evidence [32] or with the help of the Dempster–Shafer's belief (DSB) Theory, which is applied to quantify the uncertainty of estimating the forwarding reputation [46, 54].

As shown in Table 1, punishment mechanisms are incorporated in as many as half of the surveyed schemes. Most systems that incorporate a punishment component for misbehaving nodes gradually isolate the node from the entire network or from a specific network segment. Similar to punishment, some schemes consider reputation aging while updating the nodes' reputation. Time effects are introduced in the reputation/trust values of a node either to take into account the freshness of available information for reputation assessment (e.g. reputation values or forwarding evidence, depicted in Table 1 as case (a1) and case (a2), respectively), or to periodically decrease reputation values of all nodes so as to address cases where the nodes cannot verify if undelivered packets are due to misbehaving behaviour or to other reasons (case (b)). As the table indicates, reputation bootstrapping and second chance mechanisms are less frequently used. Specifically, for the determination of the initial reputation, the social characteristics of the nodes are considered in two of the surveyed schemes where reputation bootstrapping applies [44, 47]. Additionally, in [54], second chance mechanism is implicitly provided only for newcomers/users out of the specific community. In contrast, implicit or explicit social aspects (introducing in some cases new social metrics) are exploited in many social-aware cooperation enforcement schemes.

Security management is another important issue studied by the research works of Table 1. The majority of the schemes analyse the problems of cooperation enforcement when selfish and malicious nodes are present in the network. A high number of papers introduce approaches that exhibit resistance against several types of attacks including blackhole or greyhole attacks and flooding attacks. Several surveyed schemes include an identity, signature-based, mechanism for impeding potential tampering of information, efficiently addressing self-promoting and good/bad mouthing attacks. Additionally, some schemes [44, 46] address inaccurate reputation-related information provisioning through attributing a weight to the indirect recommendation provided by a witness on the behaviour of a node, which is taken equal to the trust value of the evaluator on the witness node providing the recommendation. However, this is based on the assumption that a node exhibits the same behaviour in the networking context and in the reputation mechanism itself (a good forwarder is also a good recommender and vice versa), which is not always valid. According to another approach [33], evidences of bad mouthing/good mouthing attacks may be detected by comparing a node's recommendation towards the node under evaluation with the trust

Table 1a Comparison of existing cooperation enforcement schemes exploiting a reputation system

Citation	Monitoring mechanism[a]	Direct/indirect observations	Reputation propagation	Reputation update	Reputation aging time effects
RCAR [32]	WD	direct	✗	linearly	case (b)
DTM [33]	WD	both	based on recommendations	custom formulae	case (a1)
TRSS [44]	WD	both	based on recommendations	custom formulae	✗
RADON [45]	WD PFM	both	through encounters	application of DSB theory	case (a1)
T-Prophet [46]	WD PFM	both	through encounters	application of DSB theory	Case (a2)
ironman [47]	MHE	both	through encounters	linearly	case (a1)
SUCCESS [54]	MRT	both	nodes in same community	application of DSB theory	Case (a2)
crisp [57]	MUV	both	through routing protocol	custom formulae	✗
MobiID [55]	✗	both	nodes in same community	custom formulae	case (a2)
MobiGame [37]	✗	indirect	through relay evidences	linearly	✗
iTrust [58]	MTA	indirect	through the TA	linearly	✗

[a] WD: Watchdog mechanism, WD-PFM: Watchdog (enhanced with PFMs), MHE: monitoring via history exchanges, MRT: monitoring through reputation tickets, MUV: monitoring through utility values, MTA: monitoring through TA.

Table 1b

Citation	Reputation bootstrapping	Punishment mechanism	Second chance mechanism	Social aspects	Robust against inaccurate information	Robust against collusion	Resilience against attacks[b]	Simulation environment[c]	Performance metrics
RCAR [32]	~	✗	✗	✓	~	✗	SPA, ToI	OMNeT	5
DTM [33]	✗	✗	✗	✓	✓	~	SPA BMA, GMA	NS3	3
TRSS [44]	✓	✓	✗	✓	✓	~	PTD, TB, TF	ONE	8
RADON [45]	✗	✗	✗	✗	~	✗	BA	GLM	2
T-Prophet [46]	✗	✗	✗	✗	✓	✗	BA, BMA SPA, ToI	ONE	4
ironman [47]	✓	✓	✓	✓	~	✗	✗	CUS	4
SUCCESS [54]	✗	✓	✓	✓	~	✗	BA	ONE	3
crisp [57]	✗	✗	✗	✗	✓	✓	BA, FLA	CUS	3
MobiID [55]	✗	✓	✗	✓	✓	✗	FHM	ONE	1
MobiGame [37]	✗	✓	✗	✗	✓	✗	BA, BMA FRA, CA	ONE	1
iTrust [58]	✗	✓	✗	✓	✓	✗	BA, GA	ONE	6

[b] Resilience against attacks besides selfishness; SPA: self-promoting attack, ToI: tampering of information, BMA: bad-mouthing attack, GMA: good-mouthing attack, BA: blackhole attack, FLA: flooding attack, FHM: forwarding history modification, FRA: fairness attack, CA: confidentiality attack, GA: greyhole attack.

[c] GLM: GloMoSim, CUS: custom developed simulation environment.

一定程度上 的 差别

value of the evaluator node towards the node under evaluation. If the percentage difference is higher than a threshold, it is considered suspicious and thus a negative experience. Typically, in all cases, the defence mechanisms include collaborative malicious packet detection and blacklisting of detected attackers. On the contrary, robustness against collusion is only partially touched. Overall, we believe that security in OppNets is a critical area still widely open for future research.

All surveyed cooperation enforcement schemes introduce an evaluation framework for analysing their performance. Various simulators are used to assess this performance with respect to message delivery ratio and network throughput realised, communication overhead introduced, time required for obtaining accurate reputation values, accuracy, detection time and so on. The most common simulation tools used are NS3, GloMoSim, ONE and OMNeT++ among other custom-developed simulators. Even though simulation results are provided in most of the presented works, the simulation configurations, the parameters examined and measured as well as the assumptions made, vary significantly, constituting very hard to comparatively assess the performance of the proposed schemes. However, if we consider the delivery ratio as the most important and desired metric, it is observed that the inclusion of reputation-related information enhances the exhibited performance since the impact of the presence of selfish or malicious nodes is smoothed out significantly.

Finally, although opportunistic networking has been a research topic for over a decade with a large body of theoretic work being published, there are still many research questions that need to be addressed. One of the topics that have received little to no attention is the actual scalability of OppNets. This is mostly due to the lack of large-scale test bed implementations. As a result, there exist only speculations on the levels of scalability of opportunistic networking protocols, but no real proofs on the bounds of their performance. This problem is tightly related to two more issues. First, there are the practical implications of involving a critical mass of devices to take part in controlled experiments. Second, modelling the specifics of large populations is also challenging due to the fact that these networking models often cannot be validated due to the lack of appropriate benchmarks. Accordingly, and although OppNets have been considered as a stand-alone solution, with the prediction of 50 billion connected devices by 2020 [59], it is time to discuss whether OppNets may have a larger scope in the future connected world.

6 Conclusions

Stimulating cooperation in OppNets remains a challenging endeavour so as to secure basic networking operations, such as data forwarding. Existing models that rely on traditional cryptographic techniques are considered to be complex and resource intensive, while models that either rely on Certificate Authorities/TTPs or require a certain degree of predetermined trust, are inadequate and/or difficult (even unfeasible) to be applied due to the complexity, heterogeneity, high variability and resource constraints imposed by the networking environment.

Motivated by the fact that the proposed reputation-based schemes lack unity, in the present paper, we have formed a comprehensive list of critical aspects that should be considered when designing such mechanisms. In addition, we have revisited current research efforts thoroughly discussing their distinct features, relative merits and weaknesses as well as suitable enabling technologies. In the future, we plan to continue our work towards that direction, which could hopefully form the basis for defining a unified cooperation enforcement framework for OppNets.

7 References

[1] Louta, M., Bellavista, P.: ‘Bringing always best connectivity vision a step closer: challenges and perspectives’, *IEEE Commun. Mag.*, 2013, **51**, (2), pp. 158–166

[2] Conti, M., Giordano, S.: ‘Mobile *ad hoc* networking: milestones, challenges, and new research directions’, *IEEE Commun. Mag.*, 2014, **52**, (1), pp. 85–96

[3] Liu, T., Sadler, C.M., Zhang, P., *et al.*: ‘Implementing software on resource-constrained mobile sensors: experiences with impala and zebranet’. Proc. of the 2nd Int. Conf. Mobile Systems, Applications, and Services, 2004, pp. 256–269

[4] Karaliopoulos, M., Telelis, O., Koutsopoulos, I.: ‘User recruitment for mobile crowdsensing over opportunistic networks’. 2015 IEEE Conf. Computer Communications (INFOCOM), 2015, pp. 2254–2262

[5] Louta, M., Mpanti, K., Karetsos, G., *et al.*: ‘Mobile crowd sensing architectural frameworks: a comprehensive survey’. 2016 7th Int. Conf. Information, Intelligence, Systems & Applications (IISA), 2016, pp. 1–7

[6] Khabbaz, M.J., Assi, C.M., Fawaz, W.F.: ‘Disruption-tolerant networking: a comprehensive survey on recent developments and persisting challenges’, *IEEE Commun. Surv. Tutor.*, 2012, **14**, (2), pp. 607–640

[7] Chakchouk, N.: ‘A survey on opportunistic routing in wireless communication networks’, *IEEE Commun. Surv. Tutor.*, 2015, **17**, (4), pp. 2214–2241

[8] Wei, K., Liang, X., Xu, K.: ‘A survey of social-aware routing protocols in delay tolerant networks: applications, taxonomy and design-related issues’, *IEEE Commun. Surv. Tutor.*, 2014, **16**, (1), pp. 556–578

[9] Zhu, Y., Xu, B., Shi, X., *et al.*: ‘A survey of social-based routing in delay tolerant networks: positive and negative social effects’, *IEEE Commun. Surv. Tutor.*, 2013, **15**, (1), pp. 387–401

[10] Wu, Y., Zhao, Y., Riguidel, M., *et al.*: ‘Security and trust management in opportunistic networks: a survey’, *Secur. Commun. Netw.*, 2015, **8**, (9), pp. 1812–1827

[11] Alajeely, M., Doss, R., Ahmad, A.: ‘Security and trust in opportunistic networks – a survey’, *IETE Tech. Rev.*, 2016, **33**, (3), pp. 256–268

[12] Kraounakis, S., Demetropoulos, I.N., Michalas, A., *et al.*: ‘A robust reputation-based computational model for trust establishment in pervasive systems’, *IEEE Syst. J.*, 2015, **9**, (3), pp. 878–891

[13] Li, X., Zhou, F., Yang, X.: ‘Scalable feedback aggregating (sfa) overlay for large-scale p2p trust management’, *IEEE Trans. Parallel Distrib. Syst.*, 2012, **23**, (10), pp. 1944–1957

[14] Eirinaki, M., Louta, M.D., Varlamis, I.: ‘A trust-aware system for personalized user recommendations in social networks’, *IEEE Trans. Syst. Man Cybern., Syst.*, 2014, **44**, (4), pp. 409–421

[15] Varlamis, I., Eirinaki, M., Louta, M.: ‘Application of social network metrics to a trust-aware collaborative model for generating personalized user recommendations’, *Influence Technol. Social Netw. Anal. Mining*, 2013, **6**, pp. 49–74

[16] Zhan, G., Shi, W., Deng, J.: ‘Design and implementation of tarf: a trust-aware routing framework for wsns’, *IEEE Trans. Dependable Secur. Comput.*, 2012, **9**, (2), pp. 184–197

[17] Bera, S., Misra, S., Roy, S.K., *et al.*: ‘Softwsn: software-defined wsn management system for iot applications’, *IEEE Syst. J.*, 2016, **PP**, (99), pp. 1–8

[18] Sicari, S., Rizzardi, A., Grieco, L.A., *et al.*: ‘Security, privacy and trust in internet of things: the road ahead’, *Comput. Netw.*, 2015, **76**, pp. 146–164

[19] Ruohomaa, S., Kutvonen, L.: ‘Trust management survey’, in Herrmann, P., Issarny, V., Shiu, S. (Eds): ‘*ITrust*’ (Springer, 2005), vol. **3477**, pp. 77–92

[20] Mejia, M., Peña, N., Muñoz, J.L., *et al.*: ‘A review of trust modeling in *ad hoc* networks’, *Internet Res.*, 2009, **19**, (01), pp. 88–104

[21] Azer, M., El-Kassas, S., Hassan, A., *et al.*: ‘A survey on trust and reputation schemes in *ad hoc* networks’. Third Int. Conf. Availability, Reliability and Security, 2008, ARES 08, March 2008, pp. 881–886

[22] Yu, H., Shen, Z., Miao, C., *et al.*: ‘A survey of trust and reputation management systems in wireless communications’, *Proc. IEEE*, 2010, **98**, (10), pp. 1755–1772

[23] Marias, G.F., Georgiadis, P., Flitzanis, D., *et al.*: ‘Cooperation enforcement schemes for manets: a survey’, *Wirel. Commun. Mob. Comput.*, 2006, **6**, (3), pp. 319–332

[24] Louta, M., Kraounakis, S., Michalas, A.: ‘A survey on reputation-based cooperation enforcement schemes in wireless *ad hoc* networks’. Proc. of the 2010 Int. Conf. Wireless Information Networks and Systems (WINSYS), 2010, pp. 1–4

[25] Benamar, N., Singh, K.D., Benamar, M., *et al.*: ‘Routing protocols in vehicular delay tolerant networks: a comprehensive survey’, *Comput. Commun.*, 2014, **48**, pp. 141–158

[26] Moreira, W., Mendes, P.: ‘Social-aware opportunistic routing: the new trend’, in Woungang, I., Dhurandher, S.K., Anpalagan, A., Vasilakos, A.V. (Eds): ‘*Routing in Opportunistic Networks*’ (Springer, 2013), pp. 27–68

[27] Trifunovic, S., Legendre, F.: ‘Trust in opportunistic networks’, *Comput. Eng. Netw. Lab.*, 2009, pp. 1–12

[28] Hoffman, K., Zage, D., Nita-Rotaru, C.: ‘A survey of attack and defense techniques for reputation systems’, *ACM Comput. Surv. (CSUR)*, 2009, **42**, (1), p. 1

[29] Kerr, R., Cohen, R.: ‘Smart cheaters do prosper: defeating trust and reputation systems’. Proc. of the 8th Int. Conf. Autonomous Agents and Multiagent Systems-Volume 2. Int. Foundation for Autonomous Agents and Multiagent Systems, 2009, pp. 993–1000

[30] Jøsang, A., Golbeck, J.: ‘Challenges for robust trust and reputation systems’. Proc. of the 5th Int. Workshop on Security and Trust Management (SMT 2009), Saint Malo, France, 2009, p. 52

[31] Gambetta, D., Ed.: ‘*Trust: making and breaking cooperative relations*’ (Basil Blackwell, New York, NY [UAS], 1988)

[32] Dini, G., Duca, A.L.: ‘Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network’, *Ad Hoc Netw.*, 2012, **10**, (7), pp. 1167–1178

[33] Chen, R., Bao, F., Chang, M., *et al.*: ‘Dynamic trust management for delay tolerant networks and its application to secure routing’, *IEEE Trans. Parallel Distrib. Syst.*, 2014, **25**, (5), pp. 1200–1210

[34] Resnick, P., Kuwabara, K., Zeckhauser, R., *et al.*: ‘Reputation systems’, *Commun. ACM*, 2000, **43**, (12), pp. 45–48

[35] Jiang, Q., Men, C., Yu, H., *et al.*: 'A secure credit-based incentive scheme for opportunistic networks'. 2015 7th Int. Conf. Intelligent Human-Machine Systems and Cybernetics (IHMSC), 2015, vol. **1**, pp. 87–91

[36] Sharma, A.: 'A credit based routing mechanism to contrast selfish nodes in delay tolerant networks'. 2014 Int. Conf. Parallel, Distributed and Grid Computing (PDGC), 2014, pp. 295–300

[37] Wei, L., Cao, Z., Zhu, H.: 'Mobigame: a user-centric reputation based incentive protocol for delay/disruption tolerant networks'. 2011 IEEE Global Telecommunications Conf. (GLOBECOM 2011), 2011, pp. 1–5

[38] Huang, J., Hu, Q., Bi, J., *et al.*: 'Stackelberg game based incentive mechanism for data transmission in mobile opportunistic networks'. Int. Conf. on Wireless Algorithms, Systems, and Applications, Springer, 2016, pp. 377–388

[39] Liu, Q., Liu, M., Li, Y., *et al.*: 'A novel game based incentive strategy for opportunistic networks'. 2015 IEEE Global Communications Conf. (GLOBECOM), 2015, pp. 1–6

[40] Liu, L., Yang, Q., Kong, X., *et al.*: 'Com-bis: a community-based barter incentive scheme in socially aware networking', *Int. J. Distrib. Sens. Netw.*, 2015, **11**, (8), p. 671012

[41] Gong, H., Yu, L., Zhang, X.: 'Social contribution-based routing protocol for vehicular network with selfish nodes', *Int. J. Distrib. Sens. Netw.*, 2014, **10**, (4), p. 753024

[42] Zhou, H., Chen, J., Fan, J., *et al.*: 'Consub: incentive-based content subscribing in selfish opportunistic mobile networks', *IEEE J. Sel. Areas Commun.*, 2013, **31**, (9), pp. 669–679

[43] Buchegger, S., Le Boudee, J.-Y.: 'Self-policing mobile *ad hoc* networks by reputation systems', *IEEE Commun. Mag.*, 2005, **43**, (7), pp. 101–107

[44] Yao, L., Man, Y., Huang, Z., *et al.*: 'Secure routing based on social similarity in opportunistic networks', *IEEE Trans. Wirel. Commun.*, 2016, **15**, (1), pp. 594–605

[45] Li, N., Das, S.K.: 'Radon: reputation-assisted data forwarding in opportunistic networks'. Proc. of the Second Int. Workshop on Mobile Opportunistic Networking, 2010, pp. 8–14

[46] Li, N., Das, S.K.: 'A trust-based framework for data forwarding in opportunistic networks', *Ad Hoc Netw.*, 2013, **11**, (4), pp. 1497–1509

[47] Bigwood, G., Henderson, T.: 'Ironman: using social networks to add incentives and reputation to opportunistic networks'. 2011 IEEE Third Int. Conf. Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Int. Conf. Social Computing (SocialCom), 2011, pp. 65–72

[48] Shikfa, A., Önen, M., Molva, R.: 'Privacy and confidentiality in context-based and epidemic forwarding', *Comput. Commun.*, 2010, **33**, (13), pp. 1493–1504

[49] Premalatha, S., Rajam, V.M.A.: 'Reputation management for data forwarding in opportunistic networks'. 2014 Int. Conf. IEEE Computer Communication and Informatics (ICCCI), 2014, pp. 1–7

[50] Sabater, J., Sierra, C.: 'Reputation and social network analysis in multi-agent systems'. Proc. of the First Int. Joint Conf. Autonomous Agents and Multiagent Systems: Part 1, 2002, pp. 475–482

[51] Pujol, J.M., Sangüesa, R., Delgado, J.: 'Extracting reputation in multi agent systems by means of social network topology'. Proc. of the First Int. Joint Conf. Autonomous Agents and Multiagent Systems: part 1, 2002, pp. 467–474

[52] Zhang, Y., Song, L., Jiang, C., *et al.*: 'A social-aware framework for efficient information dissemination in wireless *ad hoc* networks', *IEEE Commun. Mag.*, 2017, **55**, (1), pp. 174–179

[53] Guo, B., Yu, Z., Zhang, D., *et al.*: 'Crosscommunity sensing and mining', *IEEE Commun. Mag.*, 2014, **52**, (8), pp. 144–152

[54] Wei, L., Zhu, H., Cao, Z., *et al.*: 'Success: a secure user-centric and social-aware reputation based incentive scheme for dtns', *Ad Hoc Sens. Wirel. Netw.*, 2013, **19**, (1-2), pp. 95–118

[55] Wei, L., Zhu, H., Cao, Z., *et al.*: 'Mobiid: a user-centric and social-aware reputation based incentive scheme for delay/disruption tolerant networks'. Int. Conf. Ad-Hoc Networks and Wireless, 2011, pp. 177–190

[56] Ciobanu, R.-I., Marin, R.-C., Dobre, C., *et al.*: 'Trust and reputation management for opportunistic dissemination', *Pervasive Mob. Comput.*, 2016, **36**, pp. 44–56

[57] Sadiq, U., Kumar, M., Wright, M.: 'Crisp: collusion-resistant incentive-compatible routing and forwarding in opportunistic networks'. Proc. of the 15th ACM Int. Conf. Modeling, Analysis and Simulation of Wireless and Mobile Systems, 2012, pp. 69–78

[58] Zhu, H., Du, S., Gao, Z., *et al.*: 'A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks', *IEEE Trans. Parallel Distrib. Syst.*, 2014, **25**, (1), pp. 22–32

[59] Evans, D.: 'The internet of things: how the next evolution of the internet is changing everything', *CISCO White Paper*, 2011, **1**, (2011), pp. 1–11